View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Journal of Pure and Applied Algebra 79 (1992) 87–108
North-Holland

On the diophantine equation $x^{10} \pm y^{10} = z^2$

Stuart T. Smith

School of Mathematical Sciences, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel 69978

Communicated by A. Blass
Received 18 March 1991

Abstract

Smith, S. T., On the diophantine equation $x^{10} \pm y^{10} = z^2$, Journal of Pure and Applied Algebra 79 (1992) 87–108.

We show that the equations $x^{10} + y^{10} = z^2$ and $x^{10} - y^{10} = z^2$ have no nontrivial integral solutions. Previous demonstrations of these results depend on the fact that the equation $x^5 + y^5 = kz^5$ has no nontrivial integral solutions for $k = 1$, 2, and 8, whereas our proofs avoid this. Consequently, our proofs work in the weak fragment of arithmetic IE_1 where the results about $x^5 + y^5 = kz^5$ are not known to be available. We also show that $x^4 + 3x^2y^2 + y^4 = 5z^2$ and $x^4 - 50x^2y^2 + 125y^4 = z^2$ have no nontrivial solutions, whereas $x^4 - 3x^2y^2 + y^4 = 5z^2$ has infinitely many.

Introduction

Among the countless results relating to Fermat's last theorem there is a theorem due to Lebesgue [6] that states the following: For any natural number n, if $x^n + y^n = z^n$ has no nontrivial integral solutions, then neither does $x^{2n} + y^{2n} = z^2$. (Here 'nontrivial' means $xyz \neq 0$. See [3] for a proof of this result.) Since Fermat's last theorem is now known to hold for all n such that $3 \leq n \leq 150{,}000$ (cf. [11]), the equation $x^{2n} + y^{2n} = z^2$ has only trivial solutions for this range of n. Actually $x^4 + y^4 = z^2$ also has only trivial solutions, a result of Fermat's which can be found in any elementary number theory book and which implies Fermat's last theorem for exponent 4. We are thus led to the following conjecture, which is (presumably) weaker than Fermat's last theorem:

Conjecture 1. There are no nontrivial solutions to $x^{2n} + y^{2n} = z^2$ for $n \geq 2$.

One can consider this question in a more general setting. Logicians are interested in studying the relative strengths of various theorems in number theory.

0022-4049/92/$05.00 © 1992 – Elsevier Science Publishers B.V. All rights reserved

To do so, they look at *fragments* of arithmetic. A model of a fragment of arithmetic is a discretely ordered semiring in which induction is assumed to hold only for a restricted class of first-order formulas. (If there are no restrictions we have a model of Peano arithmetic.) For example, in the system IE_1 defined by Wilmers in [12], induction is restricted to bounded existential formulas, i.e. formulas of the form

$$\exists y_1 < t_1(\vec{x}) \cdots \exists y_n < t_n(\vec{x}) \theta(\vec{x}, y_1, \ldots, y_n),$$

where each $t_i(\vec{x}) = t_i(x_1, \ldots, x_k)$ is a polynomial in $x_1, \ldots, x_k$ with coefficients from the model, and θ is quantifier-free. Models of IE_1 exhibit many of the familiar properties of $\mathbb{N}$, e.g. the Euclidean algorithm holds, the usual properties of congruence and g.c.d. hold, all irreducibles are prime, etc. On the other hand, it is not known if the set of primes is cofinal, or if every prime has quadratic nonresidues, of if -1 is a quadratic residue of a prime p if $p \equiv 1 \bmod 4$ (for example). It is, therefore, interesting to see what kind of results about diophantine equations can be shown to hold in IE_1. In particular, we consider the equation $x^{2n} + y^{2n} = z^2$.

Now even the elementary proof of Fermat's last theorem for exponent 3 which appears in [9] uses results about quadratic reciprocity, so the proof at the beginning of this introduction is not available to us in IE_1 even for small odd values of n. However, the usual proof for $x^4 + y^4 = z^2$ carries over to IE_1, and we can adapt a proof due to Kausler ([5]; see [3]) and Kapferer [4] for $x^6 + y^6 = z^6$ to show that $x^6 + y^6 = z^2$ has no nontrivial solution in IE_1 (cf. [10]).

Similarly, Fermat's proof that $x^4 - y^4 = z^2$ has no nontrivial solutions works in IE_1. A proof for $x^6 - y^6 = z^2$ in IE_1 can be found in [10]. We speculate that this pattern continues:

Conjecture 2. There are no nontrivial solutions to $x^{2n} - y^{2n} = z^2$ for $n \geq 2$.

This conjecture is on much shakier ground than Conjecture 1, since it does not seem to follow from Fermat's last theorem for exponent n. It *does* follow (for n odd) from the statement that $x^n + y^n = kz^n$ has no nontrivial integral solutions for $k = 2$ and 2^{2n-2}. For $n = 3$ and $n = 5$ these statements are known to hold in $\mathbb{N}$ (cf. [1, pp. 70–71] and [7], respectively). Again, these results are not available to us in IE_1.

Clearly we can restrict ourselves to the case where n is prime in Conjectures 1 and 2. In this paper we show that both conjectures are provable for $n = 5$ in IE_1. However, the proofs are entirely number-theoretic, so to make them more accessible to non-logicians we work over $\mathbb{N}$ rather than in IE_1.

In Section 1 we prove that $x^{10} + y^{10} = z^2$ has only trivial solutions, and the related result that $x^4 + 3x^2y^2 + y^4 = 5z^2$ has no solutions other than those in which $x = y$. In Section 2 we prove the analogous result that $x^{10} - y^{10} = z^2$ has only trivial solutions; however, this time the equation $x^4 - 3x^2y^2 + y^4 = 5z^2$ has infinitely many nonequivalent solutions, so we instead make use of the fact that $x^4 - 50x^2y^2 + 125y^4 = z^2$ has only trivial solutions.

Both main results are based on the argument used by Kapferer in [4] to give an elementary proof of Fermat's last theorem for exponent 10; see also [10] for this result. The development here is necessarily more involved, particularly in the case of $x^{10} - y^{10} = z^2$.

1. The equation $x^{10} + y^{10} = z^2$

We begin by proving a lemma.

Lemma 1.1. *The equation* $x^4 + 3x^2y^2 + y^4 = z^2$ *has no solutions in which* $xy \neq 0$.

Proof. This is a well-known result (see [8]), but we include a proof for completeness. Since all the variables are raised to even powers we can assume they are all nonnegative, so let x, y, z be a solution with $xy \neq 0$ such that z has the minimal possible value; clearly $z > 0$. It is easy to check that x, y, z are pairwise relatively prime. Thus at least one of x, y is odd; by symmetry we can suppose y is odd.

Multiplying the given equation by 4 and rearranging gives

$$(2x^2 + 3y^2)^2 - 4z^2 = 5y^4\,. \tag{1}$$

If $5|z$, then by (1), $5|2x^2 + 3y^2$, so the left side of (1) is divisible by 25. Then $25|5y^4$, so $5|y$, contradicting $(y, z) = 1$. Therefore, $5 \nmid z$.

Factoring (1), we see that

$$(2x^2 + 3y^2 + 2z)(2x^2 + 3y^2 - 2z) = 5y^4\,. \tag{2}$$

Any common divisor of the two factors on the left-hand side of (2) must divide their difference $4z$ as well as their product $5y^4$. But $(4z, 5y^4) = 1$ because $(y, z) = 1$, $5 \nmid z$, and y is odd. Thus $(2x^2 + 3y^2 + 2z,\ 2x^2 + 3y^2 - 2z) = 1$.

By (2), then, either

$$\text{(A)} \quad 2x^2 + 3y^2 + 2z = 5a^4\,, \quad 2x^2 + 3y^2 - 2z = b^4\,,$$

or

$$\text{(B)} \quad 2x^2 + 3y^2 + 2z = b^4\,, \quad 2x^2 + 3y^2 - 2z = 5a^4\,,$$

for some a, b such that $(a, b) = 1$ and $ab = y$. In either case, adding the equations together yields

$$4x^2 + 6y^2 = 5a^4 + b^4 ,$$

so

$$4x^2 = 5a^4 - 6a^2b^2 + b^4 . \tag{3}$$

Case I: $a < b$. Then (3) factors as

$$4x^2 = (b^2 - a^2)(b^2 - 5a^2) . \tag{4}$$

Since $(b^2 - a^2) - (b^2 - 5a^2) = 4a^2$, the g.c.d. of $b^2 - a^2$ and $b^2 - 5a^2$ divides $(4x^2, 4a^2) = 4(x^2, a^2) = 4$; here $(x^2, a^2) = 1$ because $a|y$ and $(x, y) = 1$. But $y = ab$ is odd, hence so are a and b, so both $b^2 - a^2$ and $b^2 - 5a^2$ are divisible by 4. Therefore, $(b^2 - a^2, b^2 - 5a^2) = 4$, and (4) yields

$$b^2 - a^2 = 4c^2 , \qquad b^2 - 5a^2 = 4d^2 , \tag{5}$$

where $(c, d) = 1$ and $2cd = x$.

Now $b^2 \equiv a^2 \equiv 1 \bmod 8$, so the first equation in (5) implies that c is even. Thus $4c^2 \equiv 0 \bmod 16$ so $b^2 \equiv a^2 \bmod 16$. But then the second equation implies $-4a^2 \equiv 4d^2 \bmod 16$ with a odd, a contradiction. Therefore, Case I is impossible.

Case II: $a = b$. But $(a, b) = 1$ so we must have $a = b = 1$, and by (3), $x = 0$—contradiction.

Case III: $a > b$. Now (3) factors as

$$4x^2 = (a^2 - b^2)(5a^2 - b^2) .$$

Arguing as in Case I, this time we have

$$a^2 - b^2 = 4c^2 , \qquad 5a^2 - b^2 = 4d^2 . \tag{6}$$

The first equation in (6) implies that $\langle 2c, b, a\rangle$ is a primitive Pythagorean triple, so there exist p,q relatively prime such that $2c = 2pq$, $b = p^2 - q^2$, and $a = p^2 + q^2$. Substituting the last two expressions into the second equation in (6) yields

$$5(p^2 + q^2)^2 - (p^2 - q^2)^2 = 4d^2 ,$$

so

$$p^4 + 3p^2q^2 + q^4 = d^2 . \tag{7}$$

Now (7) has the same form as the original equation in the lemma, where $pq \neq 0$

because $pq = c$ and $2cd = x \neq 0$. But the fact that $2cd = x$ also implies $d < x$. Since the original equation implies $x \leq z$ we have $d < z$, contradicting the minimality of z. The lemma is thus proved. □

Since all of our equations will involve variables raised only to even powers, we will henceforth assume all variables to be nonnegative.

Next we need the following fact:

Lemma 1.2. *If* x, y, z *are pairwise relatively prime positive integers such that* $x^4 + 3x^2y^2 + y^4 = 5z^2$, *then* x, y *and* z *are all odd.*

Proof. If z is even, then x and y are odd (since $(x, z) = (y, z) = 1$); but then $x^4 + 3x^2y^2 + y^4 = 5z^2$ is odd, a contradiction. Hence *z is odd.*

At least one of x, y is also odd. The two are symmetric, so *suppose x is odd.*

We can multiply the given equation by 4 and rearrange terms to get

$$(2x^2 + 3y^2)^2 - 5y^4 = 20z^2 . \tag{8}$$

Suppose y is even, say $y = 2t$. Now $5 \nmid y$, for if $5 \mid y$, then the equation in the lemma shows that $5 \mid x$ as well, contradicting $(x, y) = 1$. Thus $5 \nmid t$; so either $t^2 \equiv 1 \bmod 5$ or else $t^2 \equiv -1 \bmod 5$. Thus at least one of $t^2 + z$, $t^2 - z$ is not divisible by 5.

(a) Suppose $5 \nmid t^2 - z$. Rewrite (8) as

$$(2x^2 + 3y^2)^2 = (2y^2 + 2z)^2 + (y^2 - 4z)^2 .$$

Substituting $y = 2t$ and simplifying, we obtain

$$(x^2 + 6t^2)^2 = (4t^2 + z)^2 + (2t^2 - 2z)^2 . \tag{9}$$

We show that $(4t^2 + z, 2t^2 - 2z) = 1$. Now

$$(4t^2 + z) - 2(2t^2 - 2z) = 5z ,$$

and

$$2(4t^2 + z) + (2t^2 - 2z) = 10t^2 .$$

Thus $(4t^2 + z, 2t^2 - 2z)$ divides $(5z, 10t^2) = 5(z, 2t^2) = 5$ since z is odd and $(z, t) = 1$, the latter holding because $t \mid y$ and $(z, y) = 1$. Therefore, $(4t^2 + z, 2t^2 - 2z) = 1$ or 5. But by our assumption, $5 \nmid t^2 - z$, so $(4t^2 + z, 2t^2 - 2z) = 1$.

By (9), then, one of $\langle 2t^2 - 2z, 4t^2 + z, x^2 + 6t^2 \rangle$ or $\langle 2z - 2t^2, 4t^2 + z, x^2 + 6t^2 \rangle$ is a primitive Pythagorean triple. In either case, there exist p and q such that

$x^2 + 6t^2 = p^2 + q^2$ with x odd. Then t *is even*, else $x^2 + 6t^2 \equiv 3 \equiv p^2 + q^2 \bmod 4$ which is impossible. On the other hand, since x and z are odd, $(x^2 + 6t^2)^2 \equiv (4t^2 + z)^2 \equiv 1 \bmod 8$, so (9) implies $4|(2t^2 - 2z)$ or $2|(t^2 - z)$. But z is odd, so therefore t *is odd* and we have a contradiction.

(b) Suppose $5 \nmid t^2 + z$. Rewrite (8) as

$$(2x^2 + 3y^2)^2 = (2y^2 - 2z)^2 + (y^2 + 4z)^2 .$$

Now substitute $y = 2t$ and argue as in (a).

We conclude that y *is odd*. □

We are now ready to prove the main result in this section.

Theorem 1.3. *The equation* $x^{10} + y^{10} = z^2$ *has no solutions in which* $xy \neq 0$.

Proof. As usual, suppose there is such a solution and take one with z minimal. Then $z > 0$ and x, y, z are pairwise relatively prime.

The given equation factors as

$$(x^2 + y^2)(x^8 - x^6y^2 + x^4y^4 - x^2y^6 + y^8) = z^2 . \tag{10}$$

We find the g.c.d. of the two factors on the left in (10). Suppose d is a common divisor of $x^2 + y^2$ and of $x^8 - x^6y^2 + x^4y^4 - x^2y^6 + y^8$. Since $(x, y) = 1$ and $d|x^2 + y^2$ we have $(x, d) = 1$. Now $x^2 \equiv -y^2 \bmod d$, so

$$x^8 - x^6y^2 + x^4y^4 - x^2y^6 + y^8 \equiv 5x^8 \equiv 0 \mod d .$$

Thus $d|5x^8$. But since $(x, d) = 1$ we must have $d|5$; therefore $d = 1$ or $d = 5$, and the g.c.d. is either 1 or 5.

(a) If the g.c.d. is 1, then (10) implies

$$x^2 + y^2 = a^2 , \qquad x^8 - x^6y^2 + x^4y^4 - x^2y^6 + y^8 = b^2 , \tag{11}$$

for some a, b relatively prime such that $ab = z$. We use a variation of Kapferer's trick in [4] and write the second equation in (11) as

$$[(x^2 - y^2)^2 + x^2y^2]^2 + x^2y^2(x^2 - y^2)^2 = b^2 ,$$

or $[s^2 + t^2]^2 + s^2t^2 = b^2$, that is,

$$s^4 + 3s^2t^2 + t^4 = b^2 ,$$

where $s = x^2 - y^2$ and $t = xy$. Since $(x, y) = 1$ we also have $(s, t) = 1$.

By Lemma 1.1, either $s = 0$ or else $t = 0$. In the former case we have $x = y$; but this implies $2x^{10} = z^2$ which is impossible since $\sqrt{2}$ is irrational. In the latter case, $t = xy = 0$, contradicting the assumption of the lemma.

(b) If the g.c.d. is 5, then (10) implies

$$x^2 + y^2 = 5a^2 , \qquad x^8 - x^6y^2 + x^4y^4 - x^2y^6 + y^8 = 5b^2 ,$$

where this time $5ab = z$. Employing the same trick as before,

$$s^4 + 3s^2t^2 + t^4 = 5b^2 ,$$

where $s = x^2 - y^2$ and $t = xy$. Since $(s, t) = 1$, clearly s, t, and b are pairwise relatively prime. By Lemma 1.2, s and t are both odd. But $x^2 - y^2$ and xy cannot both be odd, so we have a contradiction.

This proves the theorem. □

Lemma 1.2 is sufficient for part (b) of the preceding proof; however, a stronger result is true, which may be of independent interest.

Theorem 1.4. *The equation $x^4 + 3x^2y^2 + y^4 = 5z^2$ has no solutions in which $x \neq y$.*

Proof. Suppose such a solution exists and choose one making z minimal. Then $z > 0$, else $x = y = 0$. Also $x > 0$, otherwise $y^4 = 5z^2$ would imply that $\sqrt{5}$ is rational. Similarly $y > 0$. As usual, one can easily show that x, y, and z are pairwise relatively prime.

By Lemma 1.2, x, y and z are all odd. Since $x \neq y$, suppose without loss of generality that $x > y$. Then $u = (x + y)/2$ and $v = (x - y)/2$ are positive integers. Thus $x = u + v$, $y = u - v$ and the equation in the theorem becomes

$$(u + v)^4 + 3(u + v)^2(u - v)^2 + (u - v)^4 = 5z^2 ,$$

or

$$5u^4 + 6u^2v^2 + 5v^4 = 5z^2 . \tag{12}$$

Since $(x, y) = 1$ and x and y are both odd, clearly $(u, v) = 1$ (hence $(u, z) = (v, z) = 1$ as well). Then one of u,v is not divisible by 5; relabeling them if necessary, we assume $5 \nmid v$.

Multiplying (12) by 5 and rewriting,

$$(5u^2 + 3v^2)^2 + 16v^4 = 25z^2 ,$$

so

$$(5z + 5u^2 + 3v^2)(5z - 5u^2 - 3v^2) = 16v^4 . \tag{13}$$

We find the g.c.d. of the two factors on the left-hand side in (13). Their sum is $10z$ and their product is $16v^4$, so their g.c.d. divides $(10z, 16v^4) = 2(5z, 8v^4)$. Now $(z, v) = 1$, z is odd, and $5 \nmid v$, so $(5z, 8v^4) = 1$. Therefore, the g.c.d. of the two factors in (13) is 1 or 2. But their sum is $10z$ which is even, so both have the same parity. Since their product $16v^4$ is also even, $5z + 5u^2 + 3v^2$ and $5z - 5u^2 - 3v^2$ are also both even, and their g.c.d. is 2.

From (13), then, either

$$\text{(A)} \quad 5z + 5u^2 + 3v^2 = 2a^4 , \quad 5z - 5u^2 - 3v^2 = 8b^4 ,$$

or

$$\text{(B)} \quad 5z + 5u^2 + 3v^2 = 8a^4 , \quad 5z - 5u^2 - 3v^2 = 2b^4 ,$$

for some a,b such that $(a, b) = 1$ and $ab = v$.

In case (A) we subtract to obtain $10u^2 + 6v^2 = 2a^4 - 8b^4$ with $v = ab$, so

$$5u^2 = a^4 - 3a^2b^2 - 4b^4 ,$$

or

$$5u^2 = (a^2 - 4b^2)(a^2 + b^2) , \tag{14}$$

Now $4(a^2 + b^2) + (a^2 - 4b^2) = 5a^2$ and $(a, u) = 1$, so the g.c.d. of the factors on the right-hand side of (14) is 1 or 5. In either case, one of the following holds:

(i) $a^2 - 4b^2 = 5c^2$, $a^2 + b^2 = d^2$, or

(ii) $a^2 - 4b^2 = c^2$, $a^2 + b^2 = 5d^2$,

for some c, d with $(c, d) = 1$ such that either $cd = u$ or else $5cd = u$. In each case, $a^2 + b^2$ is a square modulo 4, so a and b must have opposite parity. Thus $v = ab$ is even so u odd; since $cd | u$, both c and d are also odd.

In (i), the first equation thus implies that a is odd, and so b is even. But then this equation implies $a^2 \equiv 5c^2 \bmod 8$, which is impossible for a,c odd.

In (ii), again a must be odd, and so $(a, 2b) = 1$. Thus $a^2 - (2b)^2 = c^2$ implies that $a = p^2 + q^2$, $2b = 2pq$ for some p,q of opposite parity. From the second equation

$$(p^2 + q^2)^2 + (pq)^2 = 5d^2 ,$$

or

$$p^4 + 3p^2q^2 + q^4 = 5d^2 .$$

This is of the same form as the original equation in the theorem, where $p \neq q$ because they have opposite parity. Moreover, $d|u$ so $d \leq u < z$, contradicting the minimality of z.

We can now turn to case (B). Again we subtract, this time obtaining

$$10u^2 + 6v^2 = 8a^4 - 2b^4 \quad \text{with } v = ab ,$$

or

$$5u^2 = (4a^2 + b^2)(a^2 - b^2) .$$

Again there are two possibilities:

(i) $4a^2 + b^2 = c^2$, $a^2 - b^2 = 5d^2$, or

(ii) $4a^2 + b^2 = 5c^2$, $a^2 - b^2 = d^2$,

where $(c, d) = 1$ and either $cd = u$ or else $5cd = u$. In each case, $a^2 - b^2$ is a square modulo 4; since $(a, b) = 1$, a must be odd. Then $4a^2 + b^2$ and $a^2 - b^2$ have different parities, so in each case c and d have different parities and therefore cd is even. Thus u is even so $v = ab$ is odd, hence b is odd.

In (i), since $a^2 \equiv b^2 \equiv 1 \bmod 8$ we have $5 \equiv c^2 \bmod 8$, a contradiction.

In (ii), $\langle d, b, a \rangle$ is a primitive Pythagorean triple where b is odd, hence $d = 2pq$, $b = p^2 - q^2$, $a = p^2 + q^2$ for some p, q. The first equation in (ii) implies

$$4(p^2 + q^2)^2 + (p^2 - q^2)^2 = 5c^2 ,$$

or

$$5p^4 + 6p^2q^2 + 5q^4 = 5c^2 . \tag{15}$$

Let $s = p + q$, $t = p - q$; then $2p = s + t$ and $2q = s - t$. Multiplying (15) by 16, we have

$$5(2p)^4 + 6(2p)^2(2q)^2 + 5(2q)^4 = 5(4c)^2 ,$$

and so substituting yields

$$5(s + t)^4 + 6(s + t)^2(s - t)^2 + 5(s - t)^4 = 80c^2$$

so $16s^4 + 48s^2t^2 + 16t^4 = 80c^2$, or

$$s^4 + 3s^2t^2 + t^4 = 5c^2 . \tag{16}$$

This is of the same form as the original equation in the theorem, where $s \neq t$ because $q \neq 0$ (since $d = 2pq \neq 0$). But $c|u$ so $c \leq u < z$, contradicting the minimality of z.

This proves Theorem 1.4. $\square$

The argument from equations (15) through (16) enables us to show that Theorem 1.4 implies the following:

Corollary 1.5. *The equation* $5x^4 + 6x^2y^2 + 5y^4 = 5z^2$ *has no solutions in which* $xy \neq 0$. $\square$

2. The equation $x^{10} - y^{10} = z^2$

We start with an analogue to Lemma 1.1.

Lemma 2.1. *The equation* $x^4 - 3x^2y^2 + y^4 = z^2$ *has no solutions in which* $xy \neq 0$.

Proof. This result is also cited in [8]. We suppose such a solution exists and take one with xy minimal; as usual, x,y,z will be pairwise relatively prime. Note that z is odd, since if z is even then x and y are odd, implying that $x^4 - 3x^2y^2 + y^4 = z^2$ is odd and contradicting the assumption on z. Thus $z > 0$.

Now $x = y$ is impossible since it implies $-x^4 = z^2$ and $x \neq 0$. By symmetry of x and y we can assume $x > y$. Now since $(x, y) = 1$ we have $(x^2 - y^2, xy) = 1$. Rewriting the original equation as

$$(x^2 - y^2)^2 - (xy)^2 = z^2 ,$$

we see that $\langle xy, z, x^2 - y^2 \rangle$ is a primitive Pythagorean triple. Since z is odd, we have

$$x^2 - y^2 = a^2 + b^2 , \qquad xy = 2ab , \tag{17}$$

for some a,b relatively prime and of opposite parity. Taking the first equation in (17) modulo 4 gives $x^2 - y^2 \equiv 1 \bmod 4$, so x is odd and y is even.

Let $c = (x, a)$, $d = (y, b)$; then $(c, d) = 1$ because $(x, y) = 1$. There exist r,s,t,u such that

$$x = rc , \quad a = sc , \quad y = td , \quad b = ud . \tag{18}$$

By definition of c and d, we furthermore have $(r, s) = 1$ and $(t, u) = 1$. Substituting (18) into the second equation of (17) yields

$$rctd = 2scud ,$$

or

$$rt = 2su . \tag{19}$$

Now $r|x$ and x is odd, so r is odd and therefore t is even. The fact that $(r, s) = 1$ implies from (19) that $r|2u$, hence $r|u$ since r is odd. Similarly, $t|2s$. From (19), then, we have

$$r = u , \qquad t = 2s , \tag{20}$$

so we can substitute into the first equation of (17) to get

$$(uc)^2 - (2sd)^2 = (sc)^2 + (ud)^2 ,$$

or

$$c^2(u^2 - s^2) = d^2(u^2 + 4s^2) . \tag{21}$$

Here $(c, d) = 1$ as we remarked previously, and $(u, s) = 1$ because $(a, b) = 1$. We want to find the g.c.d. of $u^2 - s^2$ and $u^2 + 4s^2$. Now

$$4(u^2 - s^2) + (u^2 + 4s^2) = 5u^2 \quad \text{and} \quad (u^2 + 4s^2) - (u^2 - s^2) = 5s^2 ,$$

where $(5u^2, 5s^2) = 5$. Thus $(u^2 - s^2, u^2 + 4s^2) = 1$ or 5.

(a) Suppose $(u^2 - s^2, u^2 + 4s^2) = 1$. Then (21) implies

$$u^2 - s^2 = d^2 , \qquad u^2 + 4s^2 = c^2 . \tag{22}$$

Now $(u, c) = 1$ because $(a, b) = 1$, so the second equation in (22) implies that $\langle 2s, u, c \rangle$ is a primitive Pythagorean triple. Therefore,

$$u = p^2 - q^2 , \qquad 2s = 2pq ,$$

for some p, q. Thus $s = pq$, and the first equation in (22) becomes

$$(p^2 - q^2)^2 - (pq)^2 = d^2 ,$$

or

$$p^4 - 3p^2q^2 + q^4 = d^2 .$$

This has the form of the equation in the lemma and $pq \neq 0$ because $s \neq 0$. But $pq = s < t \leq y \leq xy$ (the inequality $s < t$ follows from (20)), contradicting the minimality of xy.

(b) Suppose $(u^2 - s^2, u^2 + 4s^2) = 5$. Now we conclude from (21) that

$$u^2 - s^2 = 5d^2, \qquad u^2 + 4s^2 = 5c^2.$$

Solving for s^2 and u^2, respectively, yields

$$s^2 = c^2 - d^2, \qquad u^2 = c^2 + 4d^2. \tag{23}$$

As before, $(u, c) = 1$, and so this time $\langle 2d, c, u \rangle$ is a primitive Pythagorean triple. Therefore

$$c = p^2 - q^2, \qquad 2d = 2pq,$$

for some p, q. Then $d = pq$ and the first equation in (23) becomes

$$(p^2 - q^2)^2 - (pq)^2 = c^2,$$

or

$$p^4 - 3p^2q^2 + q^4 = c^2.$$

This has the form of the equation in the lemma, and $pq = d \neq 0$. But $pq = d < 2sd = td = y \leq xy$ (again using (20)), contradicting the minimality of xy. This proves the lemma. □

Next we prove a lemma similar to Lemma 1.2.

Lemma 2.2. *If x, y, and z are pairwise relatively prime positive integers such that $x^4 - 3x^2y^2 + y^4 = 5z^2$ and $x > y$, then x is even, y is odd, and z is odd.*

Proof. If z is even, then x and y are odd, so $x^4 - 3x^2y^2 + y^4 = 5z^2$ is odd, a contradiction. Therefore, *z is odd.*

We can rewrite the given equation as

$$(x^2 - y^2)^2 - (xy)^2 = 5z^2. \tag{24}$$

From the original equation we see $5|x \leftrightarrow 5|y$; since $(x, y) = 1$, we have $5 \nmid x$ and $5 \nmid y$. Thus $5 \nmid xy$, hence by (24), $5 \nmid (x^2 - y^2)$. Thus at least one of $3(x^2 - y^2) + 2xy$, $3(x^2 - y^2) - 2xy$ is not divisible by 5.

(a) Suppose $5 \nmid 3(x^2 - y^2) + 2xy$. Multiply (24) by 5 and rewrite it as

$$[3(x^2 - y^2) + 2xy]^2 - [2(x^2 - y^2) + 3xy]^2 = 25z^2.$$

Thus $\langle 2(x^2 - y^2) + 3xy, 5z, 3(x^2 - y^2) + 2xy \rangle$ is a Pythagorean triple. Moreover,

$$3[2(x^2 - y^2) + 3xy] - 2[3(x^2 - y^2) + 2xy] = 5xy$$

and $(5xy, 5z) = 5$, so the g.c.d. of the members of the triple is 1 or 5. But by assumption, $5 \nmid 3(x^2 - y^2) + 2xy$, so the g.c.d. is 1.

Since $5z$ is odd, we have $5z = p^2 - q^2$, $2(x^2 - y^2) + 3xy = 2pq$ (hence xy is even), and

$$3(x^2 - y^2) + 2xy = p^2 + q^2 , \tag{25}$$

where p and q have opposite parities. Since $2|xy$, looking at equation (25) modulo 4 gives us

$$3(x^2 - y^2) \equiv p^2 + q^2 \equiv 1 \mod 4 .$$

Thus $x^2 - y^2 \equiv 3 \bmod 4$. So x *is even* and y *is odd*.

(b) If $5 \nmid 3(x^2 - y^2) - 2xy$, multiply (24) by 5 and write the result in the form

$$[3(x^2 - y^2) - 2xy]^2 - [2(x^2 - y^2) - 3xy]^2 = 25z^2 .$$

The argument now proceeds as before. Note that $3(x^2 - y^2) - 2xy > 0$ because (24) implies $x^2 - y^2 > xy$. ($2(x^2 - y^2) - 3xy$ might be negative, in which case we replace it by $3xy - 2(x^2 - y^2)$ without affecting the argument.)

The lemma is thus proved. □

Unlike Lemma 1.2, Lemma 2.2 does not give us a contradiction at the analogous point in the proof of Theorem 2.8. If we could prove a counterpart to Theorem 1.4, we would be able to use that result instead in the argument. However, this approach will not work; the equation $x^4 - 3x^2y^2 + y^4 = 5z^2$ has infinitely many different solutions with x, y, and z relatively prime (see Corollary 2.5).

To prove this theorem, we use a general result due to Desboves [2] and quoted in [3]:

Theorem 2.3 (Desboves). *If x,y,z is a solution of $ax^4 + dx^2y^2 + by^4 = cz^2$, then so is X,Y,Z, where*

$$X = x(4bcy^4z^2 - q^2) ,$$
$$Y = y(4acx^4z^2 - q^2) ,$$
$$Z = z\{4fx^4y^4q^2 - (c^2z^4 - fx^4y^4)^2\} ;$$

here $q = ax^4 - by^4$ and $f = d^2 - 4ab$. □

Of course, there is no claim here that *all* solutions are generated in this way. Also, X,Y,Z may be negative, but from the form of the equation we can always take absolute values.

We tailor the above theorem to our specific equation and prove that the new solution generated this way really is new.

Theorem 2.4. (i) *If* x, y, z *is a solution of* $x^4 - 3x^2y^2 + y^4 = 5z^2$, *then so is* X, Y, Z, *where*

$$X = x|4y^4z^2 - \tfrac{1}{5}(x^4 - y^4)^2|\,,$$
$$Y = y|4x^4z^2 - \tfrac{1}{5}(x^4 - y^4)^2|\,,$$
$$Z = z\left|20x^4y^4\left(\frac{x^4 - y^4}{5}\right)^2 - (5z^4 - x^4y^4)^2\right|\,.$$

Moreover:

(ii) *If* $xy \neq 0$, *then* $XY \neq 0$,

(iii) *If* $(x, y) = 1$ *and* $xy \neq 0$, *then* $(X, Y) = 1$.

(iv) *If* $x > 0$, $y > 0$, $z > 0$, *then* $X > x$, $Y > y$ *and* $Z > z$.

(v) X *has the same parity as* x, Y *has the same parity as* y, *and* Z *has the same parity as* z.

(vi) *If* $x > y > 0$, *then* $X > Y > 0$.

Proof. (i) Substituting $a = b = 1$, $d = -3$, $c = 5$ (and so $q = x^4 - y^4$, $f = 5$) into Theorem 2.3, we have

$$X = x(20y^4z^2 - (x^4 - y^4)^2)\,,$$
$$Y = y(20x^4z^2 - (x^4 - y^4)^2)\,,$$
$$Z = z\{20x^4y^4(x^4 - y^4)^2 - (25z^4 - 5x^4y^4)^2\}\,.$$

We can insert absolute value signs as in the theorem. The equations in the theorem are obtained from the ones above by dividing X and Y by 5 and Z by 25; this will be legitimate once we show $5 | x^4 - y^4$.

Now from the equation in Theorem 2.4, $5|x \leftrightarrow 5|y$. So we have two cases:

(a) If $5|x$ and $5|y$, obviously $5|x^4 - y^4$.

(b) If $5 \nmid x$ and $5 \nmid y$, then $x^4 = y^4 = 1 \bmod 5$, so again $5|x^4 - y^4$. This proves (i).

For (ii)–(vi), we assume without loss of generality that $xy \neq 0$ and $x > y > 0$ (for $x = y$ implies $-x^4 = 5z^2$, so $x = y = z = 0$). Also it is easy to show that it is enough to prove (ii)–(vi) in the case where $(x, y) = 1$, so we assume this. Under these assumptions, x, y, and z are positive and pairwise relatively prime, so by Lemma 2.2, x is even and y and z are odd.

So modulo 16, $4y^4z^2 \equiv 4$ and $(x^4 - y^4)^2 \equiv (-1)^2 = 1$. Thus $\frac{1}{5}(x^4 - y^4)^2 \equiv 13 \bmod 16$, and

$$4y^4z^2 - \tfrac{1}{5}(x^4 - y^4)^2 \equiv 7 \mod 16\,. \tag{26}$$

So,

$$|4y^4z^2 - \tfrac{1}{5}(x^4 - y^4)^2| > 1 . \tag{27}$$

Similarly, $4x^2z^2 \equiv 0 \bmod 16$, and so

$$4x^4z^2 - \tfrac{1}{5}(x^4 - y^4)^2 \equiv 3 \mod 16 , \tag{28}$$

Thus,

$$|4x^4z^2 - \tfrac{1}{5}(x^4 - y^4)^2| > 1 . \tag{29}$$

Parts (ii) and (iv) of the theorem follow from (27) and (29). Part (v) follows from (26) and (28) (from which it follows that Z and z have the same parity), and (vi) follows from (iv), (v) and Lemma 2.2. (For by Lemma 2.2, if $X > Y$, then X must be even, whether or not $(X, Y) = 1$.)

Thus only (iii) remains to be proved. To show $(X, Y) = 1$, it suffices to prove four statements:

(a) $(x, y) = 1$. This is given.

(b) $(x, 4x^4z^2 - \frac{1}{5}(x^4 - y^4)^2) = 1$. In fact, we can show $(x, 20x^4z^2 - (x^4 - y^4)^2) = 1$. For if $d|x$ and $d|(20x^4z^2 - x^8 + 2x^4y^4 - y^8)$, then $d|y^8$; but $(x, y) = 1$, so $d = 1$.

(c) $(y, 4y^4z^2 - \frac{1}{5}(x^4 - y^4)^2) = 1$. As in (b).

(d) $(4x^4z^2 - \frac{1}{5}(x^4 - y^4)^2, 4y^4z^2 - \frac{1}{5}(x^4 - y^4)^2) = 1$. This is the nontrivial part. We break up the proof:

(d1) $5 \nmid z$. For $x^4 - 3x^2y^2 + y^4 = 5z^2$ is equivalent to

$$(x^2 + y^2)^2 - 5x^2y^2 = 5z^2 . \tag{30}$$

Taking (30) modulo 25, we have

$$-5x^2y^2 \equiv 5z^2 \mod 25 . \tag{31}$$

If $5|z$, then $5 \nmid xy$ because $(z, xy) = 1$. But then (31) implies $-5x^2y^2 \equiv 0 \bmod 25$, a contradiction. Thus $5 \nmid z$.

(d2) $(z, x^2 + y^2) = 1$. By (30), if $d|z$ and $d|x^2 + y^2$, then $d|5x^2y^2$. But $(z, 5x^2y^2) = 1$, by (d1) and the fact that $(z, x) = (z, y) = 1$.

(d3) $(z, x^2 - y^2) = 1$. For $x^4 - 3x^2y^2 + y^4 = 5z^2$ implies

$$(x^2 - y^2)^2 - x^2y^2 = 5z^2 .$$

Since $(z, xy) = 1$, this implies $(z, x^2 - y^2) = 1$.

(d4) $(4x^4z^2, (x^4 - y^4)^2) = 1$. Since $x^4 - y^4$ is odd by Lemma 2.2, then

$(4, (x^4 - y^4)^2) = 1$. Also $(x^4, (x^4 - y^4)^2) = 1$ because $(x, y) = 1$. Finally, $(z, x^4 - y^4) = 1$ by (d2) and (d3), so $(z^2, (x^4 - y^4)^2) = 1$.

Now we can prove (d). Suppose d is a common divisor of $4x^4z^2 - \frac{1}{5}(x^4 - y^4)^2$ and of $4y^4z^2 - \frac{1}{5}(x^4 - y^4)^2$. By (d4), $(d, 4x^4z^2) = 1$ and $(d, (x^4 - y^4)^2) = 1$, so $(d, 4z^2(x^4 - y^4)) = 1$. But

$$d|[4x^4z^2 - \tfrac{1}{5}(x^4 - y^4)^2] - [4y^4z^2 - \tfrac{1}{5}(x^4 - y^4)^2],$$

i.e. $d|4z^2(x^4 - y^4)$. Therefore, $d = 1$. □

Corollary 2.5. *The equation $x^4 - 3x^2y^2 + y^4 = 5z^2$ has infinitely many solutions with x, y, z pairwise relatively prime.*

Proof. By Theorem 2.4, it suffices to find one such solution with $xy \neq 0$. But $x = 2$, $y = 1$, $z = 1$ is such a solution. (Theorem 2.4 then generates the next solution $X = 82$, $Y = 19$, $Z = 2759$, etc.) □

Having shown that our previous plan of action fails, we need an alterative argument, which depends on the following lemma:

Lemma 2.6. *The equation $x^4 - 50x^2y^2 + 125y^4 = z^2$ has no solutions in which $y \neq 0$.*

Proof. Suppose there is such a solution and choose one making xy minimal. Then $x > 0$, else $125y^4 = z^2$ which implies $\sqrt{125} = 5\sqrt{5}$ is rational. Also $z > 0$, otherwise $(x^2 - 25y^2)^2 = 500y^4$, implying that $\sqrt{500} = 10\sqrt{5}$ is rational.

We show that x, y, and z are pairwise relatively prime. The argument is routine except for the possibility that $5|x$ and $5|z$; we must show that this implies $5|y$. So suppose $x = 5u$, $z = 5v$. Then

$$625u^4 - 1250u^2y^2 + 125y^4 = 25v^2 . \tag{32}$$

Thus $25v^2 \equiv 0 \bmod 125$, so $5|v$ (hence $25|z$). Now (32) implies $125y^4 \equiv 0 \bmod 625$, so $5|y$ as required. Since $25|z$, we can divide the equation in the lemma by 625 and obtain a similar equation. This contradicts the minimality of xy.

Since $5|x \leftrightarrow 5|z$, the fact that $(x, z) = 1$ implies $5 \nmid x$ and $5 \nmid z$.

Next, we show that z is odd. For if z is even then x and y are odd. Taking our equation modulo 16, we have

$$x^4 - 2x^2y^2 - 3y^4 \equiv z^2 \mod 16 , \tag{33}$$

where $x^4 \equiv y^4 \equiv 1 \bmod 16$ and $x^2y^2 \equiv 1$ or $9 \bmod 16$. Thus $-2x^2y^2 \equiv -2 \bmod 16$, so (33) implies $-4 \equiv z^2 \bmod 16$ which is impossible.

Now since $5 \nmid x$ we have $x \neq 5y$, so there are two possibilities.

(i) *Suppose* $x > 5y$. Write the equation of the lemma as

$$(x^2 - 25y^2)^2 - z^2 = 500y^4 ,$$

or

$$(x^2 - 25y^2 + z)(x^2 - 25y^2 - z) = 500y^4 . \tag{34}$$

We find the g.c.d. of the factors on the left-hand side of (34). Their difference is $2z$ and their product is $500y^4$, so their g.c.d. divides $(2z, 500y^4) = 2(z, 250y^4) = 2$ because $(z, y) = 1$, z is odd, and $5 \nmid z$. So the g.c.d. of $x^2 - 25y^2 + z$ and $x^2 - 25y^2 - z$ is either 1 or 2. But they have the same parity and their product is even, so they are both even and their g.c.d. is therefore 2.

Hence by (34), we have either

$$\text{(A)} \quad x^2 - 25y^2 + z = 2a^4 , \qquad x^2 - 25y^2 - z = 250b^4 ,$$

or

$$\text{(B)} \quad x^2 - 25y^2 + z = 250b^4 , \quad x^2 - 25y^2 - z = 2a^4 ,$$

for some a,b such that $(a, b) = 1$ and $y = ab$. In either case, adding the equations together gives us $2x^2 - 50y^2 = 2a^4 + 250b^4$ with $y = ab$; thus

$$x^2 = a^4 + 25a^2b^2 + 125b^4 . \tag{35}$$

We can deduce from (35) that x is odd. For if x is even, then since $(x, a) = (x, b) = 1$ we must have a,b odd; but then (35) implies that x is odd. Since z is also odd, $y = ab$ must be even. Multiplying (35) by 4 and rearranging, $4x^2 = (2a^2 + 25b^2)^2 - 125b^4$ so

$$(2a^2 + 25b^2 + 2x)(2a^2 + 25b^2 - 2x) = 125b^4 . \tag{36}$$

We find the g.c.d. of the factors on the left in (36). Their difference is $4x$ and their product is $125b^4$, so their g.c.d. divides $(4x, 125b^4)$. Now x is odd and $5 \nmid x$; since $(x, b) = 1$, then $(4x, 125b^4)$ is 1 if b is odd and 4 if b is even.

(a) If b is odd, the above implies that the g.c.d. of the factors on the left in (36) is 1. Then either

$$\text{(A)} \quad 2a^2 + 25b^2 + 2x = c^4 , \qquad 2a^2 + 25b^2 - 2x = 125d^4 ,$$

or

$$\text{(B)}\quad 2a^2+25b^2+2x=125d^4\,,\quad 2a^2+25b^2-2x=c^4\,,$$

where $(c, d)=1$ and $cd=b$. In either case, adding yields

$$4a^2+50b^2=c^4+125d^4 \quad \text{with } b=cd\,,$$

so

$$(2a)^2=c^4-50c^2d^2+125d^4\,. \tag{37}$$

This has the form of the equation in the lemma, but we do not need to use infinite descent here. Simply note that since $(c, d)=1$, our previous proof that z is odd shows that (37) has no solution.

(b) If b is even, the g.c.d. of the factors in (36) divides 4. But in this case a is odd; since x is odd, both factors in (36) are divisible by 4, so their g.c.d. equals 4. By (36), either

$$\text{(A)}\quad 2a^2+25b^2+2x=4c^4\,,\qquad 2a^2+25b^2-2x=500d^4\,,$$

or

$$\text{(B)}\quad 2a^2+25b^2+2x=500d^4\,,\quad 2a^2+25b^2-2x=4c^4\,,$$

where $(c, d)=1$ and $b=2cd$. In either case, adding yields

$$4a^2+50b^2=4c^4+500d^4 \quad \text{with } b=2cd\,,$$

so

$$a^2=c^4-50c^2d^2+125d^4\,. \tag{38}$$

This time we do need infinite descent. Equation (38) has the same form as the equation in the lemma and $d \neq 0$, but $cd<2cd=b\leq ab=y\leq xy$, which contradicts the minimality of xy.

This completes the argument in the case $x>5y$. We continue with:

(ii) *Suppose* $x<5y$. This time we write the equation of the lemma in the form

$$(25y^2-x^2)^2-z^2=500y^4\,,$$

or

$$(25y^2-x^2+z)(25y^2-x^2-z)=500y^4\,. \tag{39}$$

The same argument as that following (34) shows that the g.c.d. of the two factors on the left in (39) is 2. Therefore, by (39) we have either

$$\text{(A)}\quad 25y^2 - x^2 + z = 2a^4\,, \qquad 25y^2 - x^2 - z = 250b^4\,,$$

or

$$\text{(B)}\quad 25y^2 - x^2 + z = 250b^4\,, \quad 25y^2 - x^2 - z = 2a^4\,,$$

where $(a, b) = 1$ and $y = ab$. In either case, adding gives

$$50y^2 - 2x^2 = 2a^4 + 250b^4\,,$$

or

$$25y^2 - x^2 = a^4 + 125b^4\,, \tag{40}$$

where x is odd and $y = ab$ is even (as we noted after equation (35)); thus one of a,b is even and the other odd. However, $25y^2 - x^2 \equiv -1 \bmod 4$ whereas $a^4 + 125b^4 \equiv a^4 + b^4 \equiv 1 \bmod 4$. Hence (40) gives us a contradiction. Thus $x < 5y$ cannot occur, and Lemma 2.6 is proved. □

For the record, we note that the above proof enables us to show the following:

Corollary 2.7. *The equation $x^4 + 25x^2y^2 + 125y^4 = z^2$ has no solution in which $y \neq 0$.*

Proof. Suppose such a solution exists. Since $125y^4 = z^2$ has no solution for $y \neq 0$, we must have $x \neq 0$ as well; take $x > 0$, $y > 0$. Writing the equation as

$$(2x^2 + 25y^2)^2 - 4z^2 = 125y^4\,,$$

we see that if $z = 0$, then $125y^4$ is a square, which is impossible. Therefore, $z > 0$.

By an argument similar to that in Lemma 2.6, we can take x,y,z pairwise relatively prime. In particular, $5 \nmid x$ and $5 \nmid z$.

Note that x and y cannot both be odd, else the equation in the corollary implies $3 \equiv z^2 \bmod 4$.

We can now use the argument from (35) onward to show that z is odd and to reduce the equation in the corollary to the one in Lemma 2.6. □

Now we can prove that Conjecture 2 holds when $n = 5$.

Theorem 2.8. *The equation $x^{10} - y^{10} = z^2$ has no solutions in which $yz \neq 0$.*

Proof. Suppose there is such a solution; clearly we can take x,y,z pairwise relatively prime. Note $x \neq 0$.

The given equation factors as:

$$(x^2 - y^2)(x^8 + x^6y^2 + x^4y^4 + x^2y^6 + y^8) = z^2 . \tag{41}$$

By an argument similar to that following (10), the g.c.d. of the factors in (41) is 1 or 5.

(a) If the g.c.d. is 1, then since $z \neq 0$,

$$x^2 - y^2 = a^2 , \qquad x^8 + x^6y^2 + x^4y^4 + x^2y^6 + y^8 = b^2 , \tag{42}$$

for some a,b such that $(a, b) = 1$ and $ab = z$. By Kapferer's trick in [4], the second equation in (42) is

$$[(x^2 + y^2)^2 - x^2y^2]^2 - x^2y^2(x^2 + y^2)^2 = b^2 ,$$

or

$$[s^2 - t^2]^2 - s^2t^2 = b^2 ,$$

that is

$$s^4 - 3s^2t^2 + t^4 = b^2 ,$$

where $s = x^2 + y^2$ and $t = xy$.

By Lemma 2.1, either $s = 0$ or $t = 0$; however, both possibilities imply $xy = 0$. Now if $x = 0$, so are y and z, so in any case $y = 0$. This was all under the assumption that $z \neq 0$; thus we conclude $yz = 0$.

(b) If the g.c.d. of the factors in (41) is 5, then since $z \neq 0$,

$$x^2 - y^2 = 5a^2 , \qquad x^8 + x^6y^2 + x^4y^4 + x^2y^6 + y^8 = 5b^2 , \tag{43}$$

for some a,b such that $(a, b) = 1$ and $z = 5ab$.

We will show that the second equation in (43) has no solution in which $x \neq y$. By the same argument as in (a), this equation becomes

$$s^4 - 3s^2t^2 + t^4 = 5b^2 \tag{44}$$

with $s = x^2 + y^2$ and $t = xy$. Since $(x, y) = 1$ we have $(s, t) = 1$, so s, t, and b are pairwise relatively prime.

Now $x \neq y$ so $(x - y)^2 > 0$, hence $x^2 + y^2 > 2xy$. In particular, $s > t$, so by Lemma 2.2, s is even, t is odd, and b is odd. Therefore, x and y are both odd, so

$u = (x + y)/2$ and $v = (x - y)/2$ are positive integers. Furthermore, one is even and one is odd, and $(u, v) = 1$ because $(x, y) = 1$. Substituting $x = u + v$, $y = u - v$ into the second equation in (43) leads to an involved computation which eventually yields

$$5u^8 + 60u^6v^2 + 126u^4v^4 + 60u^2v^6 + 5v^8 = 5b^2 . \tag{45}$$

This can be rewritten as

$$5(u^4 + 6u^2v^2 + v^4)^2 - 5b^2 = 64u^4v^4 ,$$

or

$$5[(u^4 + 6u^2v^2 + v^4 + b)(u^4 + 6u^2v^2 + v^4 - b)] = 4(2uv)^4 . \tag{46}$$

The difference of the two factors in the square brackets is $2b$ and their product divides $64u^4v^4$, so we compute $(2b, 64u^4v^4) = 2(b, 32u^4v^4)$. Now from (45) we see that if $(u, b) > 1$, then u, v, and b have a common factor, contradicting $(xy, z) = 1$. (We rely here on the fact that (44) and the proof after (30) show that $5 \nmid b$.) Thus $(u, b) = 1$ and similarly $(v, b) = 1$. Also b is odd, so $2(b, 32u^4v^4) = 2$. Therefore, the g.c.d. of the two factors in the square brackets in (46) is 1 or 2. However, they have the same parity and their product is even, so both are even and their g.c.d. is 2.

From equation (46) we have the following two possibilities:

$$\text{(A)} \quad u^4 + 6u^2v^2 + v^4 + z = 2c^4 , \qquad u^4 + 6u^2v^2 + v^4 - z = 2 \cdot 5^3 d^4 ,$$

or

$$\text{(B)} \quad u^4 + 6u^2v^2 + v^4 + z = 2 \cdot 5^3 d^4 , \quad u^4 + 6u^2v^2 + v^4 - z = 2c^4 ,$$

for some c,d such that $(c, d) = 1$ and $5cd = 2uv$. In either case, we can add the equations together and get

$$2u^4 + 12u^2v^2 + 2v^4 = 2c^4 + 250d^4 ,$$

or

$$u^4 + 6u^2v^2 + v^4 = c^4 + 125d^4 .$$

Subtracting $8u^2v^2$ from each side, we have

$$u^4 - 2u^2v^2 + v^4 = c^4 - 2(2uv)^2 + 125d^4 ,$$

or

$$(u^2 - v^2)^2 = c^4 - 50c^2d^2 + 125d^4 , \tag{47}$$

since $2uv = 5cd$.

By Lemma 2.6, equation (47) has no solutions in which $d \neq 0$. This contradiction completes the proof. □

In part (b) of the preceding proof, we showed the following result:

Corollary 2.9. *The equation* $x^8 + x^6y^2 + x^4y^4 + x^2y^6 + y^8 = 5z^2$ *has no solutions in which* $x \neq y$.

References

[1] R.D. Carmichael, Diophantine Analysis (Wiley, New York, 1915).
[2] A. Desboves, Nouv. Ann. Math. (2) 18 (1879) p. 440.
[3] L.E. Dickson, History of the Theory of Numbers, Vol. II: Diophantine Analysis (Chelsea, New York, 1952).
[4] H. Kapferer, Archiv. Math. Phys. 3 (21) (1913) 143–146.
[5] C.F. Kausler, Nova Acta Acad. Sc. Petrop. 15 (1806), ad annos 1799–1802, 146–155.
[6] V.A. Lebesgue, J. de Math. 5 (1840) 184–185.
[7] V.A. Lebesgue, J. de Math. 8 (1843) 49–70.
[8] L.J. Mordell, Diophantine Equations (Academic Press, London, 1969).
[9] W. Sierpinski, Elementary Theory of Numbers (PWN, Warsaw, 1964).
[10] S.T. Smith, Fermat's last theorem and Bezout's theorem in GCD domains, J. Pure Appl. Algebra 79 (1) (1992) 63–85 (this issue).
[11] J.W. Tanner and S.S. Wagstaff Jr, Math. Comp. 48 (1987) 341–350.
[12] G. Wilmers, Bounded existential induction, J. Symbolic Logic 50 (1) (1985) 72–90.